NACDL - Fourth Amendment

18-23 minutes

The Fourth Amendment and its guarantees should not turn on the medium used to transmit private information, nor on how the information is stored. NACDL strives to guarantee that evidence obtained in violation of the Fourth Amendment is excluded in a court of law.

Below, you can find a wide range of resources that we provide on Fourth Amendment issues.

Continue reading below

Supported by NFCJ

The NACDL Foundation for Criminal Justice preserves and promotes the core values of the National Association of Criminal Defense Lawyers and the American criminal justice system.

Support Us Now

Featured

Read Now: Coalition Letter to Senate Judiciary on Online Service Providers Reporting Drug Sales

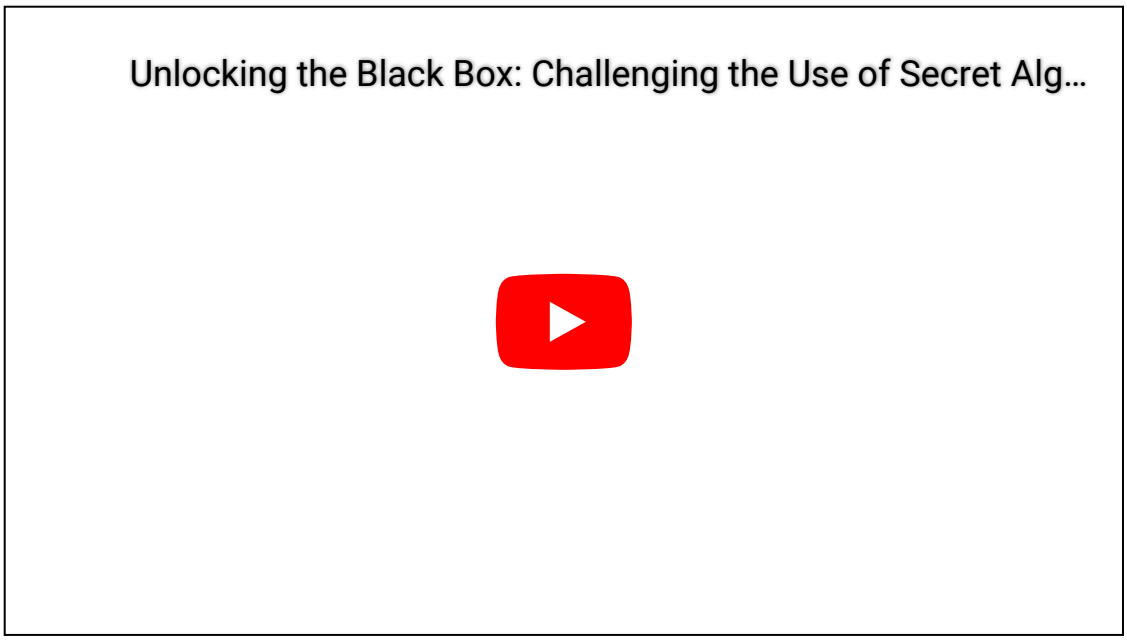
NACDL opposes the Cooper Davis Act. The bill purports to address the sale of methamphetamine, fentanyl, and "counterfeit substances" by coopting online services to report the alleged or suspected creation, manufacture, or distribution of these substances … Rather than meaningfully addressing the public health crisis caused by such substances, this bill would … undermin[e] the Fourth Amendment and the Stored Communications Act, likely with disproportionate effects on people of color, LGBTQ+ people, and other marginalized communities.

"When It Comes To Email, Some Prisoners Say Attorney-Client Privilege Has Been Erased"

"It's a staple on some of the longest-running crime shows on television: Communications between people charged with crimes and their lawyers are protected from government snooping under what's known as attorney-client privilege. In practice, things don't always work that way, especially when it comes to email messages between incarcerated people in the federal system and their attorneys. That's because within the Federal Bureau of Prisons, inmates are asked to 'voluntarily' agree to electronic monitoring in order to use the bureau's email system. The National Association of Criminal Defense Lawyers says there's nothing voluntary about it. Unless incarcerated people agree to monitoring, they're locked out of email communications. The group and a prominent civil liberties clinic at the University of California, Berkeley are now sounding the alarm. They say their concerns have been compounded during a pandemic that has made in-person visits particularly risky."

Read the full story on NPR here.

Watch Now: "Unlocking the Black Box: Challenging the Use of Secret Algorithms and Technologies in Criminal Cases" Webinar



How can criminal defense attorneys understand and confront the limitations of software-based evidence and machine learning algorithms in criminal proceedings? From probabilistic genotyping to “risk assessment” software, the recent explosion of emerging technologies has transformed almost every aspect of the criminal legal system. Increasing amounts of data and evidence are being interrogated and generated using software systems that are kept from defense teams, the courts, and the general public. The assertion of “trade secrets” by the companies who develop these tools deprive defense lawyers of access to information on how the software was constructed and the opportunity to assess its accuracy, credibility and reliability. This program guided defense attorneys through the challenges of obtaining “black box” evidence and confronting the flaws, bugs, and biases embedded in technologies deployed in the criminal justice system.

Find the rest of our video trainings here.

How to Fix the Internet: "Fixing a Digital Loophole in the Fourth Amendment"

Jumana Musa, Director of the Fourth Amendment Center, recently joined the Electronic Frontier Foundation's podcast *How to Fix the Internet* to discuss discuss how the third-party doctrine is undermining our Fourth Amendment right to privacy when we use digital services, and how recent court victories are a hopeful sign that we may reclaim these privacy rights in the future.

The recording and transcript of the podcast can be found here.

Preserving Incarcerated Persons’ Attorney-Client Privilege in the 21st Century: Why the Federal Bureau of Prisons Must Stop Monitoring Confidential Legal Emails

This new report by NACDL and the Samuelson Clinic makes the case for Congress to act immediately to protect the attorney-client privilege in emails sent between attorneys' offices and people in BOP custody. It also calls for the BOP to stop its practice of requiring incarcerated clients to “voluntarily” agree that their email will be monitored and that attorney-client privilege will not apply to legal emails, just as the government is required to in other contexts.

The full report can be found here.

NACDL Files Amicus Brief in State v. Jackson (2019)

NACDL has filed an amicus brief with American Civil Liberties Union of New Jersey and the Association of Criminal Defense Lawyers of New Jersey, arguing that prosecutors wishing to listen in on calls a defendant makes from jail must first get a warrant. This is in support of the State v. Jackson case (Superior Court of New Jersey; Case No. 083286), which argued that defendant Mark Jackson had a reasonable expectation of privacy in the calls he made to his mother from jail. Jackson did not forfeit all privacy rights in his telephone conversations by exposing them to jail staff for security monitoring purposes. Requiring prosecutors to secure warrants in order to access jail calls is the only adequate way to protect the constitutional and policy interests the calls implicate.

Read: Letter to Members of Congress on Protecting Attorney-Client Communications in BOP Custody

Coalition letter to members of Congress from NACDL and other concerned organizations regarding the need to ensure privileged communication between attorneys and clients in BOP custody, as addressed in the Effective Assistance of Counsel in the Digital Era Act (H.R. 546, 2021).

Read the joint letter here.

Read: Letter to President Biden on Need to Address Discriminatory and Militarized Policing

Coalition letter to President Biden regarding the absence thus far of executive actions addressing discriminatory and militarized policing in Black and Brown communities.

Read the joint letter here.

Read: Joint Letter from NACDL and the Due Process Institute on Constitutional and Privacy Issues in the EARN IT Act of 2020 (S. 3398)

"The bill is intended to address the sexual exploitation of children online, which is a serious and pressing issue. However, the measures proposed will create constitutional issues that reach far beyond their stated purpose. In particular, we are writing to address issues that would create or exacerbate existing problems in the criminal justice system."

Read the joint letter here.

Read Coalition Letter: NACDL Urges Senators to Change "USA FREEDOM Reauthorization Act of 2020" (H.R. 6172) to Protect Privacy

"In the four years since the USA FREEDOM Act was passed, several revelations have made clear that the FISA authorities in question lack sufficient safeguards for Constitutional rights, and that agencies have not even complied with the safeguards that exist. Such sweeping surveillance authorities that have repeatedly been shown to violate privacy rights should not be passed without open debate and opportunity for amendment."

Read the coalition letter here.

If a device is locked or encrypted, can law enforcement compel a suspect to unlock or decrypt it? Read NACDL's primer on this emerging issue.

> Can the government force someone to decrypt a digital device? Encryption is as omnipresent as computers, tablets and smartphones, yet the Supreme Court has not ruled on the constitutional implications of compelled decryption orders. The Fourth Amendment Center has published a Compelled Decryption Primer that outlines the state of the law and offers guidance for lawyers litigating this important emerging issue. The realities of modern technology require a rethinking of old doctrines to adequately safeguard constitutional rights into the future. Using this primer, attorneys can educate themselves on the basics of compelled decryption and come equipped with arguments and cases when confronting a decryption order.

Read "Split Over Compelled Decryption Deepens With Massachusetts Case" by Michael Price and Zach Simonetti, featured in *Just Security*.

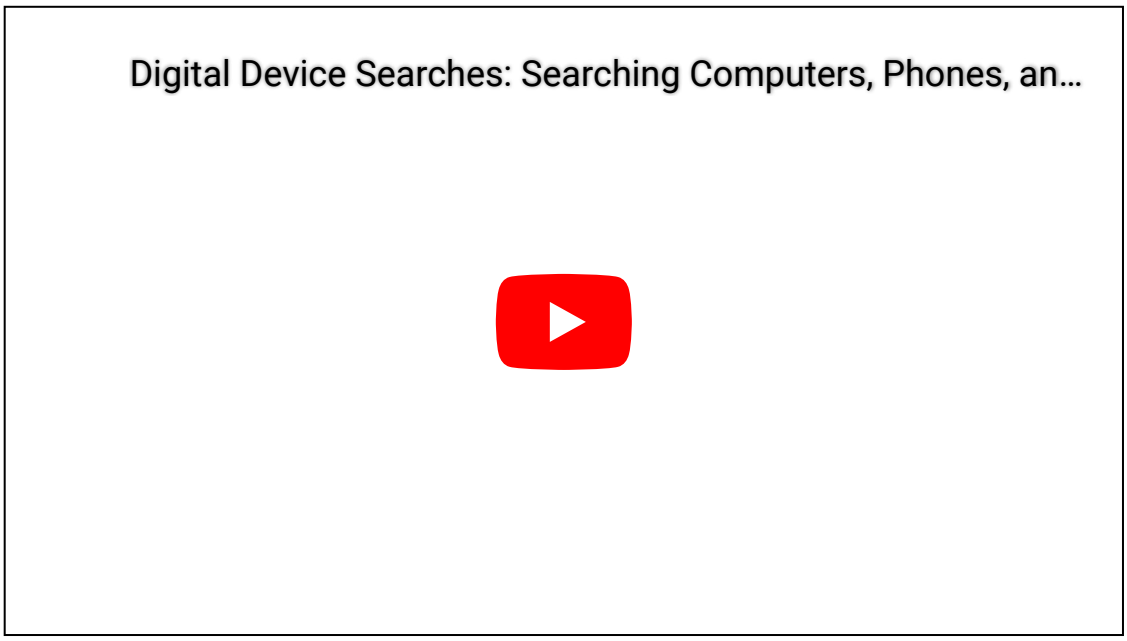
> "It has been almost a decade since Apple first offered encryption on iPhones, but the legal fight over compelled decryption remains a pitched battle. A recent volley saw the Massachusetts Supreme Judicial Court double down on the wrong side of recurring litigation over when, if ever, the government can force someone to decrypt a digital device that has been seized pursuant to a valid search warrant. As encryption winds its way into the U.S. Supreme Court's vocabulary, defense lawyers and advocates should pay careful attention to these developments – and be prepared to confront them in court."

Combatting the Surveillance State in Criminal Proceedings

This two-day CLE conference discussed the government's use of technologically advanced investigative techniques in criminal cases, and the issues raised by those techniques under

the Fourth Amendment and other federal law.

Advanced technologies are revolutionizing how the government investigates, charges and prosecutes criminal cases—and defense attorneys must keep pace. Even small police departments can purchase powerful surveillance technologies, and internet companies collect vast troves of data on virtually everyone. This CLE was co-sponsored by NACDL and the Berkeley Center for Law and Technology (BCLT), and held at International House, the University of California - Berkeley from November 29 to 30, 2018.



All of the videos from the conference are free and can be viewed in this playlist.

The Future of the Fourth Amendment

"Building on Carpenter: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider" by Michael Price, Senior Litigation Counsel, and Bill Wolf, member of NACDL's Board of Directors and NACDL's Fourth Amendment Advocacy Committee.

> "The implications of the Supreme Court's decision in *Carpenter v. United States* are just now coming into view as lower courts begin to apply Carpenter's lessons to other forms of modern surveillance. [...] This article offers a snapshot of some current investigative techniques that may be ripe for constitutional challenges in a post-*Carpenter* world."

Read "Concealing Evidence: 'Parallel Construction,' Federal Investigations, and the Constitution," written by Natasha Babazadeh and published in the Fall 2018 issue of the *Virginia Journal of Law and Technology.*

> "Federal law enforcement agencies are increasingly relying on “parallel construction" to pursue criminal cases against U.S. persons. Parallel construction is the process of building a separate — and parallel — evidentiary basis for a criminal investigation. The process is undertaken to conceal the original source of evidence, which may have been obtained unlawfully. Clandestinely used for decades, this process raises serious constitutional questions."

The June 2018 issue of *The Champion* featured "Carpenter v. United States and the Future Fourth Amendment" by Michael Price, Senior Litigation Counsel.

> "The Supreme Court's recent opinion in Carpenter v. United States has set a course for rethinking Fourth Amendment rights in the digital age. It is the third bright star in the last seven years, marking a welcome and long overdue departure from the so-called 'third-party doctrine' that has limited privacy rights for the last four decades. In a 5-4 decision, the Court ruled that police must usually get a warrant to access historical 'cell site location information' (CSLI) — geographic data held by a cellphone service provider about where a device has connected to its network. It is a major win for privacy rights and it

shines the way forward for future Fourth Amendment challenges: digital is different. The question becomes, different how? And how far might Carpenter extend?"

Facial Recognition Webinar

On September 18, NACDL held a free webinar about the practices, risks, and limitations of emerging facial recognition technology. With an increasing number of police departments across the country turning to unregulated, untested, and flawed facial recognition technology to identify suspects, it is vital defenders understand the technology, its limitations, and how to challenge its use in their cases. This webinar explored these issues with the Georgetown Law Center of Privacy and Technology's **Clare Garvie,** Bronx Defender's **Kaitlin Jackson**, and computer scientist **Joshua Kroll**. This webinar was supported by Grant No. 2013-MU-BX-K014 awarded by the Bureau of Justice Assistance.

Location Privacy after *Carpenter*

On July 2, 2018, the Center on Privacy and Technology at Georgetown Law and the Fourth Amendment Center at the National Association of Criminal Defense Lawyers hosted a forum discussing location and cell phone privacy after the Supreme Court ruling in *Carpenter v. United States.*

The Supreme Court held, in a 5-4 decision, that law enforcement agencies are required to obtain a warrant when accessing historic cell site location information. Featuring the insight of privacy experts and seasoned litigators, the discussion explored both the broad implications of the landmark ruling and the practical ramifications on future litigation.

Parallel Construction Webinar

On May 23, 2018, NACDL held a free webinar about the practice of government evidence laundering, known as “parallel construction." When the U.S. government launders the origin of evidence obtained in criminal cases, it is able to obscure secret surveillance technology or potentially unconstitutional investigative methods from the accused in criminal cases. The webinar featured **Brian Pori**, a federal public defender from New Mexico with extensive experience leading trainings on government evidence laundering, and **Sarah St. Vincent**, the author of Human Rights Watch's comprehensive investigative report “Dark Side: Secret Origins of Evidence in US Criminal Cases."

Protecting Your Digital Devices at the Border

U.S. Customs and Border Protection (CBP) searches the digital devices of people at border crossings and at ports of entry without a warrant and without suspicion. NACDL members are uniquely exposed to abuse in this context: digital devices store materials and information subject to the attorney-client privilege and attorney work-product doctrine, as well as information on overseas clients and witnesses, and other extremely sensitive materials that could be covered by Rule 1.6 of the Model Rules of Professional Responsibility.

The webinar was presented by **Esha Bhandari**, a staff attorney with the ACLU Speech, Privacy, and Technology Project, where she focuses on litigation and advocacy relating to online speech, academic freedom, privacy rights, and the impact of big data.

Read "Protecting Your Digital Devices at the Border: A Criminal Defense Lawyer's Primer" here and find the companion case list here.

This primer aims to educate attorneys about the implications of CBP's claimed powers and offer strategies that will help them comply with their ethical obligations and responsibilities to their clients when entering the U.S. Along with the primer, NACDL compiled a resource of district court cases that deal with the border search exception and digital devices, with special attention paid to the influence of *Riley v. California*.

CBP updates directive on border searches of digital devices

On January 4, 2018, Customs and Border Protection (CBP) released a directive on the border searches of digital devices that made significant changes to the practices that NACDL detailed in “Protecting Your Digital Devices at the Border: A Criminal Defense Lawyer's Primer." The directive includes specific procedures to protect attorney-client privilege and work product doctrine, as well as a dangerous new provision that asserts travels have an "obligation" to provide CBP with their device passwords. You can learn more about the directive from Esha Bandari at the ACLU, the Deeplinks blog at the Electronic Frontier Foundation, and Edward Hasbrouck's two-part analysis of the password provision.

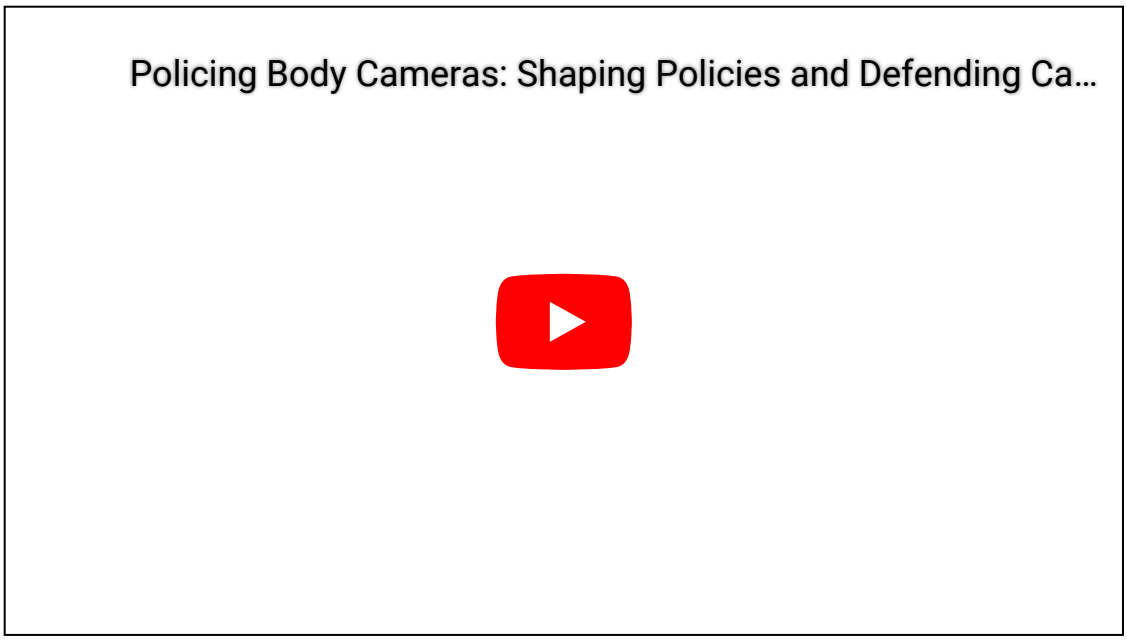
Challenging Government Hacking in Criminal Cases

NACDL hosted a webinar featuring the expertise of **Colin Fieman**, an Assistant Federal Public Defender and lead counsel in the first “Operation Pacifier" cases, and **Paul Ohm**, a law professor and specialist in information privacy, computer crime law, intellectual property, and criminal procedure.

NACDL also published a guide on challenging evidence seized by government-installed computer malware, authored by the American Civil Liberties Union with input from NACDL and the Electronic Frontier Foundation.

The guide, “Challenging Government Hacking in Criminal Cases," examines recent court decisions on the government's use of malware in the context of Fourth Amendment protections from unreasonable searches.

Body Camera Webinar



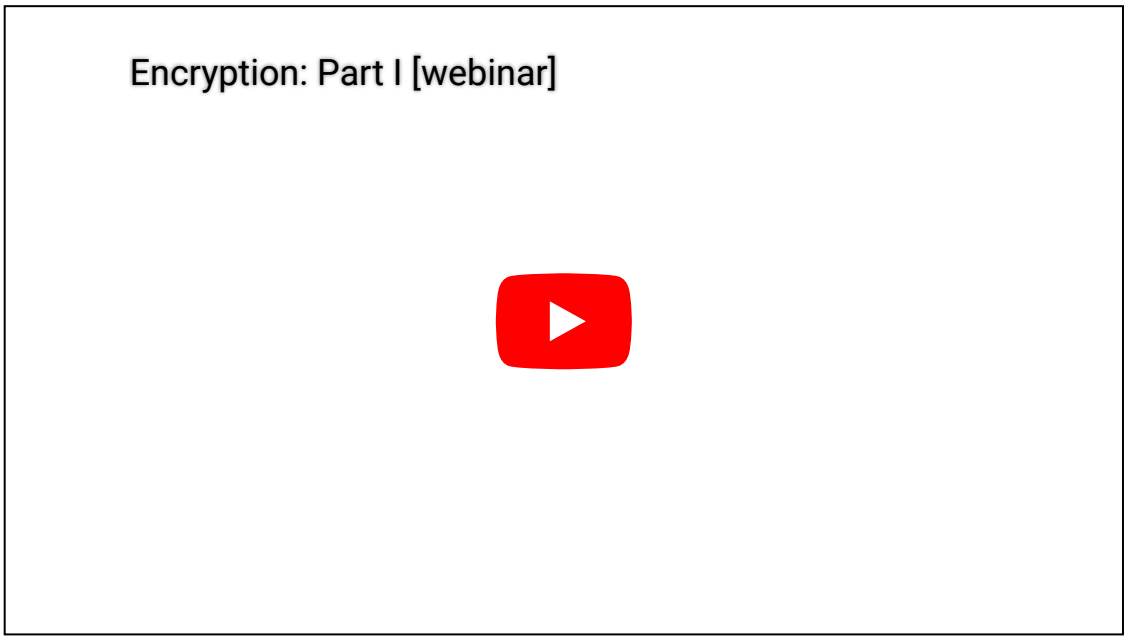
This webinar walks through the recommendations and talks about how to negotiate stronger body camera policies in your jurisdiction, the technical aspects of body cameras, and strategies and tactics for defending clients in body camera jurisdictions.

This report outlines NACDL's position on the introduction and use of body cameras by law enforcement.

Encryption Webinar

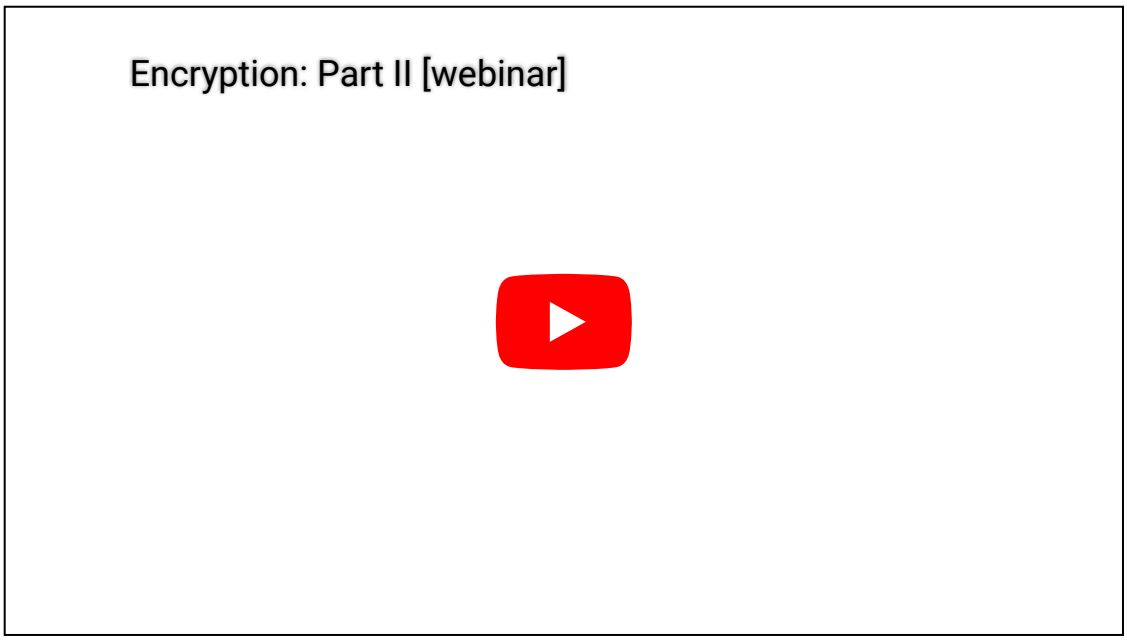
Watch "Keep It Confidential: Protecting Your Privileged Client Communications with Encryption"

Defense lawyers regularly use phone calls, texts, and emails to communicate with clients, investigators, witnesses and others associated with their cases. Many of these communications are privileged, yet government surveillance programs can capture and store them. This webinar explored how this happens, and how defense lawyers can keep their communications out of government hands.



During the first part of the webinar, **Jack Gillum**, reporter on The Associated Press's Washington investigations team, addressed his experience with encrypting communications and why he and others in his industry have made the switch to these encrypted platforms. **Neema Singh Guliani**, Legislative Counsel at the American Civil Liberties

Union, then laid out the different surveillance programs and technologies that may be intercepting your privileged communications.



During the second part of the webinar, **Harlo Holmes**, Digital Security Trainer with the Freedom of the Press Foundation, walked through some basic ways to encrypt phone calls, texts, and email communications.
